# IBE and S/MIME

**Russ Housley**

Founder of Vigil Security, LLC

Chair of IETF

V<sup>igil</sup>

S<sub>ecurity</sub> <sub>LLC</sub>

---

# Adding New Algorithms

- Algorithm standards are just the beginning
- Modern security protocols are algorithm agile, but each protocol needs to be profiled to use each algorithm
- Innovative new algorithms may require the use of protocol extensions or support infrastructure to take advantage of unforeseen capabilities
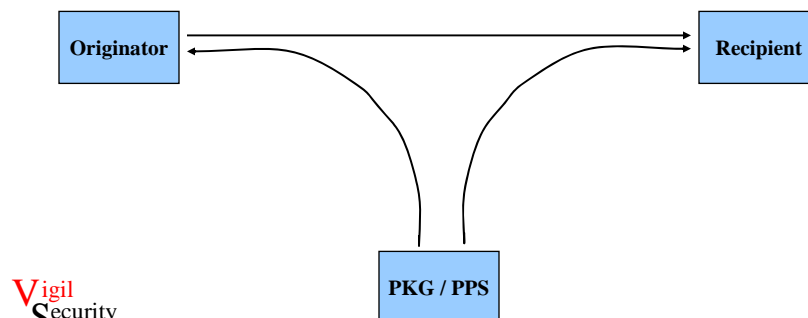
V<sup>igil</sup>

S<sub>ecurity</sub> <sub>LLC</sub>

# Traditional S/MIME Encryption

1. Originator fetches the certificate
   (or saves it from an earlier message)
2. Originator sends the encrypted message

| Originator | → | Recipient |

**Certificate Repository**
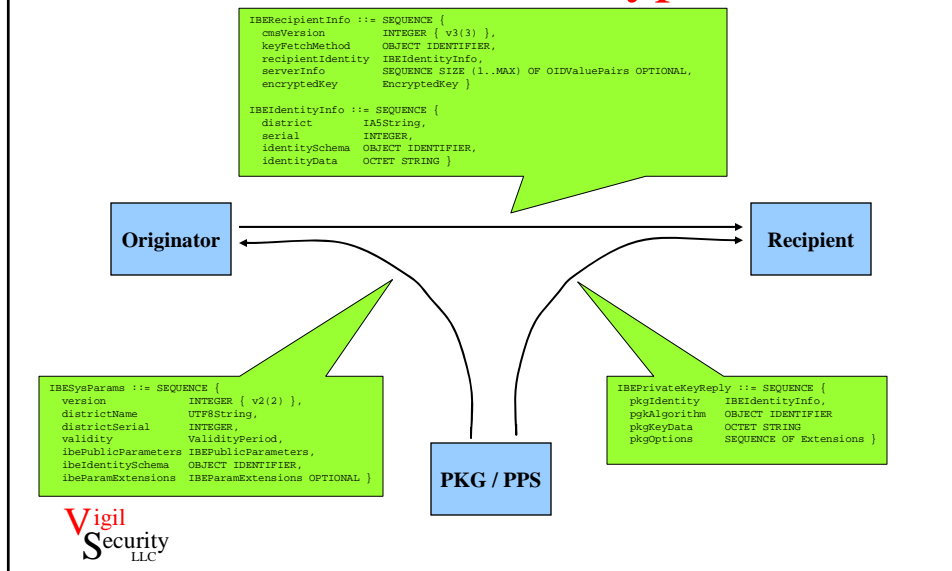
**V**igil **S**ecurity LLC

---
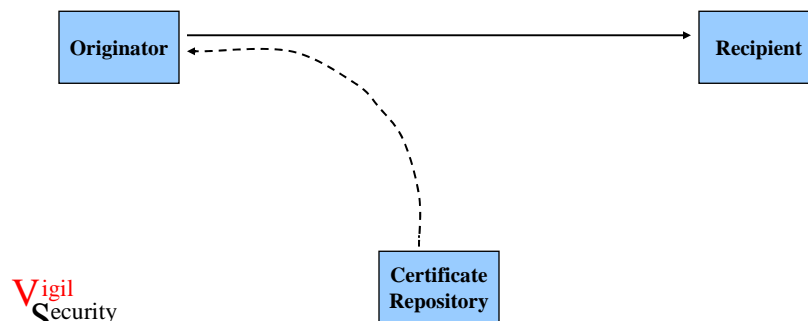
# IBE S/MIME Encryption

1. Originator fetches the IBE Public Parameters
2. Originator sends the encrypted message
3. Recipient fetches their IBE private key

| Originator | ⇄ | Recipient |

**PKG / PPS**

**V**igil **S**ecurity LLC

# IBE S/MIME Encryption

```
IBERecipientInfo ::= SEQUENCE {
  cmsVersion          INTEGER { v3(3) },
  keyFetchMethod      OBJECT IDENTIFIER,
  recipientIdentity   IBEIdentityInfo,
  serverInfo          SEQUENCE SIZE (1..MAX) OF OIDValuePairs OPTIONAL,
  encryptedKey        EncryptedKey }

IBEIdentityInfo ::= SEQUENCE {
  district        IA5String,
  serial          INTEGER,
  identitySchema  OBJECT IDENTIFIER,
  identityData    OCTET STRING }
```

**Originator**

**Recipient**

```
IBESysParams ::= SEQUENCE {
  version             INTEGER { v2(2) },
  districtName        UTF8String,
  districtSerial      INTEGER,
  validity            ValidityPeriod,
  ibePublicParameters IBEPublicParameters,
  ibeIdentitySchema   OBJECT IDENTIFIER,
  ibeParamExtensions  IBEParamExtensions OPTIONAL }
```

```
IBEPrivateKeyReply ::= SEQUENCE {
  pkgIdentity   IBEIdentityInfo,
  pgkAlgorithm  OBJECT IDENTIFIER
  pkgKeyData    OCTET STRING
  pkgOptions    SEQUENCE OF Extensions }
```

**PKG / PPS**

Vigil Security LLC

---

# Interoperability is the Goal

- Interoperable use of new algorithms means:
  - Algorithm standards
  - Specification of syntax and elements of procedure to use the new algorithm in existing security protocols

Vigil Security LLC

# Questions?

Russ Housley
housley@vigilsec.com

Vigil
Security
LLC